Bobby Saadian, SBN 250377
ClassAction@wilshirelawfirm.com
Justin F. Marquez, SBN 262417
justin@wilshirelawfirm.com
Thiago M. Coelho, SBN 324715
thiago@wilshirelawfirm.com
Robert J. Dart, SBN 264060
rdart@wilshirelawfirm.com
WILSHIRE LAW FIRM
3055 Wilshire Blvd., 12th Floor
Los Angeles, California 90010
Telephone: (213) 381-9988
Facsimile: (213) 381-9989

Attorneys for Plaintiff and Proposed Class Counsel

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

LAVARIOUS GARDINER, individually and on behalf of all others similarly situated, Plaintiff, v. WALMART INC., a Delaware corporation; DOES 1 to 10, inclusive, Defendants.	CASE NO.: **CLASS ACTION** **COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiff Lavarious Gardiner, individually, and on behalf of all others similarly situated, brings this action based upon his personal knowledge as to himself and his own acts, and as to all other matters upon information and belief, based upon, *inter alia*, the investigation of his attorneys.

NATURE OF THE ACTION

1. Defendant Walmart, Inc. ("Walmart") is a retailer selling goods at its stores and online via its website. Hundreds of millions of customers shop at Walmart every week. Those customers reasonably expect the highest level of protection for their private identifiable

information (referred to collectively as, "PII") when giving highly sensitive information, including credit card numbers, to Walmart, when creating Walmart accounts for shopping online. What Walmart customers do not expect is that their personal and sensitive information, including access to their credit card accounts, will be harvested by unauthorized individuals. And yet that is precisely what has happened, with millions of Walmart accounts available for sale on the dark web.

2. Plaintiff, individually, and on behalf of those similarly situated persons (hereafter, "Class Members"), brings this class action to secure redress against Defendants for their reckless and negligent violation of customer privacy rights. Plaintiff and Class Members are individuals who were customers of Walmart during the four year period prior to the date of the filing of this Complaint to the present.

3. Plaintiff and Class Members suffered significant injuries and damages. The security breach compromised the full names, addresses, financial account information, credit card information, and other private identifiable information of Walmart's customers.

4. As a result of Defendants' wrongful actions and inactions, unauthorized individuals gained access to and harvested Plaintiff's and Class Members' PII. Walmart's website's vulnerabilities led to direct breaches of Walmart's systems, and led hackers to be able to attack Walmarts' customers' computers directly as well. Plaintiff has been forced to take remedial steps to protect himself from future loss. Indeed, all Class Members are currently at a very high risk of identity theft and/or credit fraud, and prophylactic measures, such as the purchase of credit monitoring services and software, are reasonable and necessary to prevent and mitigate future loss.

5. As a result of Defendants' wrongful actions and inactions, customer information was stolen. Many customers of Walmart have had their PII compromised, have had their privacy rights violated, have been exposed to the risk of fraud and identify theft, and have otherwise suffered damages.

///

///

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

6. Further, despite the fact that the accounts are available for sale on the dark web, and Walmart's website contains multiple severe vulnerabilities through which the data was obtained, Walmart has failed whatsoever to notify its customers that their data has been stolen.

THE PARTIES

7. Plaintiff Lavarious Gardiner is a California citizen residing in San Francisco, California. Plaintiff is a customer of Walmart who gave his PII to Walmart, a necessary step in the creation of a Walmart account. Plaintiff is informed and believes that his PII was accessed by hackers as a direct result of the data breach that took place at Walmart. Thus, Plaintiff's account was compromised. Plaintiff's Walmart account, and all of the data it contains, is currently being sold on the dark web. Consequently, as a necessary and reasonable measure to protect himself, Plaintiff purchased a credit and personal identity monitoring service to alert him to potential misappropriation of his identity and to combat risk of further identity theft. At a minimum, therefore, Plaintiff has suffered compensable damages because his data is being sold on the dark web, and he has been forced to purchase a credit monitoring service, a reasonable and necessary prophylactic step to prevent and mitigate future loss. Exposure of Plaintiff's PII as a result of the Walmart data breach has placed him at imminent, immediate and continuing risk of further identity theft-related harm.

8. Defendant Walmart is a Delaware corporation with its principal place of business located in Bentonville, Arkansas.

9. Plaintiff is unaware of the true names, identities, and capacities of the defendants sued herein as DOES 1 to 10. Plaintiff will seek leave to amend this complaint to allege the true names and capacities of DOES 1 to 10 if and when ascertained. Plaintiff alleges, upon information and belief, that each of the defendants sued herein as a DOE is legally responsible in some manner for the events and happenings alleged herein, and, as set forth below, that each of the defendants sued herein as a DOE proximately caused injuries and damages to Plaintiff and Class Members.

///

///

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

10. As used herein, "Defendants" shall refer to Walmart and Does 1 to 10, collectively.

JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction over the state law claims asserted herein pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), since some of the Class Members are citizens of a State different from the Defendant; there are more than 100 putative class members; and the amount in controversy exceeds $5,000,000.

12. The Court also has personal jurisdiction over the parties because, on information and belief, Defendants conduct a major part of their national operations with regular and continuous business activity in California, through a large number of stores and with an advertising budget not exceeded in other jurisdictions throughout the United States. Plaintiff's and the Class Members' claims arise out of Defendants' business activity in California because Plaintiff's and the Class Members created Walmart accounts in California, and because Plaintiff's and the Class Members' California Walmart accounts were hacked.

13. Venue is appropriate in this District because, among other things: (a) Defendant directed its activities at residents in this District; and (b) many of the acts and omissions that give rise to this Action took place in this judicial District.

FACTUAL ALLEGATIONS

A. Walmart's Data Breach

14. Walmart is a major American retailer, operating numerous stores and selling goods via its website. Purchasers at Walmart create Walmart accounts, which store their personal information, including credit card information. Walmart has been the target of many successful hacks. The hackers obtain access to Walmart accounts by hacking Walmart's website and Walmart's customers' computers, using vulnerabilities on Walmart's website, and subsequently posting the stolen accounts on the dark web for sale.

15. That Walmart has been successfully hacked is illustrated by the fact that the dark web is replete with stolen Walmart accounts for sale. Over two million accounts are available for sale at websites such as http://wwhclubl4tefzrzf.onion/index.php?threads/skupaju-gifty-amazon-carters-walmart-old-navy-pod-vysokij.58790/page-12, and

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

http://blackpasqk3nqfuc.onion/shopps. Many similar websites exist. Plaintiff successfully identified many specific persons by name and address information provided by these websites, including himself.

16. Moreover, Plaintiff retains in his possession communications with the hackers in which they state that the accounts they are selling are real accounts that belong to Walmart customers.

17. Further, the fact that Walmart's systems are quite vulnerable to a hack evidences that Walmart was hacked. A scan of Walmart's domains using Open Web Application Security Project Zed Attack Proxy ("OWASP ZAP"), which is widely used in the cybersecurity community to scan websites for documented vulnerabilities, resulted in the exposure of six major vulnerabilities.

18. These vulnerabilities include:

- There were seven instances of private IP addresses being disclosed in the public website code. While this is not a direct attack vector, it may contribute to an attack on Walmart's systems.
- There were 44 instances of password autocomplete enabled. This could potentially contribute to a hacker's breach of a user's account. If a script or malware is running on the client's computer, the script or malware can extract the password from the browser.
- The cookie "No HttpOnlyFlag" being set, which means that cookies can be accessed by scripts or malware on the client machine. This can be used to conduct session hijacking attacks. If the customer has malware on his or her computer, that malware can manipulate and access cookie data.
- There were 8,615 instances of cross-site scripting ("XSS") protection not enabled. This is a very serious issue, which means that the site could be vulnerable to the common cross site scripting attack. In such an attack, the hacker injects client-side script into web pages which are viewed by other users, typically targeting areas in which there is a high level of user interaction. When the user interacts with those

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

areas, the website executes the attacker's script rather than the intended website functionality. This would enable the hacker to steal account information from the customers.

- There were 100,061 instances of Cross Domain JavaScript source file inclusion. This would also allow a hacker to perform cross site scripting, by inserting malicious JavaScript.
- There were 93,060 instances of a cookie without the secure flag being set. This is similar to the No HttpOnlyFlag being set, in that it enables cookies to be accessed through unencrypted connections.

19. An OWASP Zap scan of http://grocery.walmart.com and the IP address for Walmart photos revealed similar vulnerabilities on those websites.

20. Scans using other highly respected vulnerability scanners resulted in affirmation of the aforementioned vulnerabilities, and the finding of additional vulnerabilities which hackers can take advantage of to obtain protected files from a website. For example, a scan of less than 2% of the Walmart website using the Vega vulnerability scanner uncovered 228 high ranked vulnerabilities. These vulnerabilities include the integer overflow vulnerability, and numbers exposed which appeared to be social security numbers and credit card numbers. Vega also found seven instances where local paths were revealed, which can allow hackers to obtain sensitive information about the server environment.

21. Plaintiff also conducted a scan of the website using the Nessus tool. Government agencies that use the Nessus tool to scan websites include the IRS, Argonne National Lab, Defense Information Systems Agency, Department of Defense, U.S. Navy, and others. Plaintiff utilized the Nessus PCI scan. PCI stands for Payment Card Industry, and the Nessus PCI scan tests the website against the PCI DSS standards, which organizations must follow if they accept payment cards from major credit card brands. A company that is not PCI complaint can be fined and, in some cases, their payment card privileges can be revoked. Defendant is not PCI compliant. The scan showed 20 PCI vulnerabilities, each ranked as high, and identified the following severe

///

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

issues, each of which would be considered to be an "automatic failure," according to the PCI DSS Approved Scanning Vendors Program Guide (version 3.1):

- Vulnerabilities with a CVSS base score greater than or equal to 4.0;
- Unsupported operating systems;
- Internet reachable database servers;
- Presence of built-in or default accounts;
- Unrestricted DNS Zone transfers;
- Unvalidated parameters leading to SQL injection attacks;
- XSS flaws;
- Directory traversal vulnerabilities;
- HTTP response splitting/header injection;
- Detection of backdoor applications (malware, trojan horses, rootkits, backdoors)
- Use of older, insecure SSL/TLS versions
- Use of anonymous key exchange protocols (such as anonymous Diffe-Hellman in SSL/TLS);
- Scan Interference.

22. The Nessus PCI scan also located three problems with Walmart.com's SSL/TLS certificates. SSL/TLS stands for Secure Sockets Layer/Transport Layer Security and is how websites encrypt data transmissions. SSL/TLS utilizes digital certificates to encrypt data. Security flaws in SSL/TLS certificates make all transmissions vulnerable, including transmissions of credit card information and account details.

23. The Nessus PCI scan identified the following problems with Walmart.com's SSL/TLS certificates: SSL certificate cannot be trusted, SSL certificate with wrong hostname, and SSL self-signed certificate. Each of these problems means that data transmissions on the website are vulnerable.

24. The Nessus PCI scan also revealed that Defendant is using an outdated protocol, TLS Version 1.1, which is technology that was replaced 12 years ago and has known weaknesses.

///

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

C. California Recognizes the Importance of PII

25. *California Civil Code* § 1798.81.5(a)(1) states that: "It is the intent of the Legislature to ensure that personal information about California residents is protected. To that end, the purpose of this section is to encourage businesses that own, license, or maintain personal information about Californians to provide reasonable security for that information."

D. Stolen Information Is Valuable to Hackers and Thieves

26. It is well known, and the subject of many media reports, that PII is highly coveted and a frequent target of hackers. Especially in the technology industry, the issue of data security and threats thereto is well known. Despite well-publicized litigation and frequent public announcements of data breaches, Defendants maintained an insufficient and inadequate system to protect the PII of Plaintiff and Class Members.

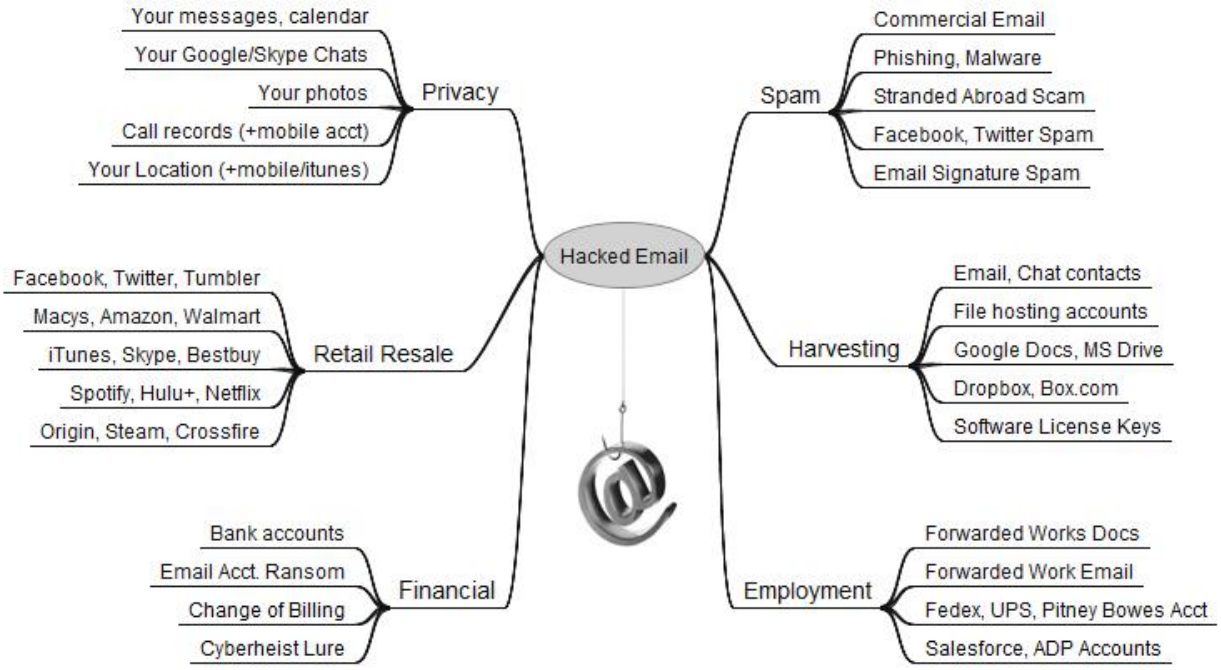
27. Legitimate organizations and members of the criminal underground alike recognize the value of PII. Otherwise, they would not aggressively seek and pay for it. As previously seen in one of the world's largest data breaches, hackers compromised the card holder data of 40 million of Target's customers. *See* "Target: 40 million credit cards compromised," CNN Money, Dec. 19, 2013, *available* at http://money.cnn.com/2013/12/18/news/companies/target-credit-card/**.** In contrast, DataCoup provides just one example of a legitimate business that pays users for personal information. *See* http://money.com/money/3001361/datacoup-facebook-personal-data-privacy/.

28. PII is highly valuable to hackers. Identity thieves use stolen PII for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud. PII that is stolen from the point of sale are known as "dumps." *See* Krebs on Security April 16, 2016, Blog Post, *available at* https://krebsonsecurity.com/2016/04/all-about-fraud-how-crooks-get-the-cvv/. PII can be used to clone a debit or credit card. *Id.*

29. Once someone buys PII, it is then used to gain access to different areas of the victim's digital life, including bank accounts, social media, and credit card details. During that process, other sensitive data may be harvested from the victim's accounts, as well as from those belonging to family, friends, and colleagues.

30. In addition to PII, a hacked email account can be very valuable to cyber criminals. Since most online accounts require an email address not only as a username, but also as a way to verify accounts and reset passwords, a hacked email account could open up a number of other accounts to an attacker.[1]

31. As shown below, a hacked email account can be used by an identity thief to link to many other sources of information, including any purchase or account information found in the hacked email account.[2]



32. Hacked information can also enable thieves to obtain other personal information through "phishing." According to the Report on Phishing available on the United States, Department of Justice's website: "AT&T, a large telecommunications company, had its sales system hacked into, resulting in stolen order information including full names and home addresses, order numbers, and credit card numbers. The hackers then sent each customer a highly personalized e-mail indicating that there had been a problem processing their order and re-

[1] Identity Theft and the Value of Your Personal Data, Trend Micro (Apr. 30, 2015), https://www.trendmicro.com/vinfo/us/security/news/online-privacy/identity-theft-and-the-value-of-your-personal-data.

[2] Brian Krebs, The Value of a Hacked Email Account, Krebs on Security (June 13, 2013, 3:14 PM), https://krebsonsecurity.com/2013/06/the-value-of-a-hacked-email-account/.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

directing them to a spoofed website where they were prompted to enter further information, including birthdates and Social Security numbers."[3]

E. The Data Breach Has Resulted and Will Result in Identity Theft and Identity Fraud

33. Defendants failed to implement and maintain reasonable security procedures and practices appropriate to protect the PII of Plaintiff and Class Members.

34. The ramifications of Defendants' failure to keep Plaintiff's and Class Members' PII secure is severe. According to Javelin Strategy and Research, "one in every three people who is notified of being a potential fraud victim becomes one . . . with 46% of consumers who had cards breached becoming fraud victims that same year." "Someone Became an Identity Theft Victim Every 2 Seconds Last Year," Fox Business, Feb. 5, 2014 *available* at http://www.foxbusiness.com/personal-finance/2014/02/05/someone-became-identitytheft-victim-every-2-seconds-last-year.html.

35. In the case of a data breach, simply reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, after conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems." *See* "Victims of Identity Theft," U.S. Department of Justice, Dec 2013, *available at* https://www.bjs.gov/content/pub/pdf/vit12.pdf. In fact, the BJS reported, "resolving the problems caused by identity theft [could] take more than a year for some victims." *Id*. at 11.

36. A person whose PII has been obtained and compromised may not know or experience the full extent of identity theft or fraud for years. It may take some time for the victim to become aware of the theft or fraud. In addition, a victim may not become aware of fraudulent charges when they are nominal because typical fraud-prevention algorithms fail to capture such charges. Those charges may be repeated, over and over again, on a victim's account, without notice for years.

///

[3] https://www.justice.gov/archive/opa/docs/report_on_phishing.pdf

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

F. Annual Monetary Losses from Identity Theft are in the Billions of Dollars

37. According to the BJS, an estimated 17.6 million people were victims of one or more incidents of identity theft in 2014. Among identity theft victims, existing bank or credit card accounts were the most common types of misused information. *Id*.

38. Javelin Strategy and Research reports that losses from identity theft reached $21 billion in 2013. *See* 2013 Identity Fraud Report, attached hereto as **Exhibit A**. There may be a time lag between when harm occurs and when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO, Report to Congressional Requesters, at 33 (June 2007), *available at* http://www.gao.gov/new.items/d07737.pdf.

39. As a result of the data breach, Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiff and Class Members are also subject to a higher risk of phishing and pharming where hackers exploit information they already obtained in an effort to procure even more PII. Plaintiff and Class Members are presently incurring and will continue to incur such damages, in addition to any fraudulent credit and debit card charges incurred by them, and the resulting loss of use of their credit and access to funds, whether or not such charges are ultimately reimbursed by the credit card companies. In addition, Plaintiff and Class Members now run the risk of unauthorized individuals creating credit cards in their names, taking out loans in their names, and engaging in other fraudulent conduct using their identities.

G. Plaintiff and Class Members Suffered Damages

40. The exposure of Plaintiff's and Class Members' PII to unauthorized third-party hackers was a direct and proximate result of Defendants' failure to properly safeguard and protect

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

Plaintiff's and Class Members' PII from unauthorized access, use, and disclosure, as required by their common law duty of care, which is informed by federal standards. The data breach was a result of Defendants' failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class Members' PII in order to protect against reasonably foreseeable threats to the security or integrity of such information, also required by their federal standards.

41. Plaintiff's and Class Members' PII is private and sensitive in nature and was inadequately protected by Defendants. As a direct and proximate result of Defendants' wrongful actions and inaction and the resulting data breach, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing risk of harm from identity theft and identity fraud, requiring them to take the time and effort to mitigate the actual and potential impact of the subject data breach on their lives by, among other things, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring their credit reports and accounts for unauthorized activity.

42. Defendants' wrongful actions and inactions directly and proximately caused the theft and dissemination of Plaintiff's and Class Members' PII into the public domain, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. The improper disclosure, compromise, and theft of their PII;

b. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of unauthorized third-party hackers and misused via the sale of Plaintiff's and Class Members' information on the Internet black market;

c. The nonexistent notification of the data breach;

d. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the data breach;

e. Ascertainable losses in the form of deprivation of the value of their PII, for which there is a well-established national and international market; and

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

g. Overpayments to Defendants for the goods bought from Defendant, as it was understood that a portion of that price would be applied to the costs of implementing reasonable and adequate safeguards and security measures that would protect their PII, which Defendants failed to implement. As a result, Plaintiff and Class Members did not receive what they paid for and were overcharged by Defendants.

CLASS ACTION ALLEGATIONS

43. Plaintiff bring this action on his own behalf and on behalf of a class of individuals pursuant to Rule 23 of the Federal Rules of Civil Procedure. Plaintiff intends to seek certification of a class defined as follows:

> All persons residing in the State of California who had a Walmart account at any time from four years prior to the date of the filing of this Complaint to the date of notice is sent to the class (the "Class").

44. Excluded from the Class are: (a) Defendants, including any entity in which any of the Defendants has a controlling interest, is a parent or a subsidiary of, or which is controlled by any of the Defendants; (b) the officers, directors, and legal representatives of Defendants; and (c) Plaintiff's counsel, the judge, and the court personnel in this case, as well as any members of their immediate families. Plaintiff reserves the right to amend the definition of the Class if discovery, further investigation and/or rulings by the Court dictate that it should be modified.

45. *Numerosity*. The members of the Class are so numerous that the joinder of all Class Members is impractical. While the exact number of Class Members is unknown to Plaintiff at this time, given the number of Walmart customers in California, it stands to reason that the number of Class Members is at least in the thousands. Class Members are readily identifiable from information and records in Defendants' possession, custody, or control, such as account information.

46. *Commonality and Predominance*. This action involves questions of law and fact common to Class Members that predominate over any questions affecting individual Class Members. These common questions of law and fact include, without limitation:

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

a. Whether Defendants owed a duty of care to Plaintiff and Class Members with respect to the security of their PII;

b. What security measures must be implemented by Defendants to comply with their duty of care;

c. Whether Defendants met the duty of care owed to Plaintiff and the Class Members with respect to the security of the PII;

d. The nature of the relief, including equitable relief, to which Plaintiff and Class Members are entitled; and

e. Whether Plaintiff and Class Members are entitled to damages, civil penalties and/or injunctive relief.

47. *Typicality*. Plaintiff's claims are typical of those of other Class Members because Plaintiff's PII, like that of each of the other Class Members, was exposed and/or improperly disclosed by Defendants.

48. *Adequacy of Representation*. Plaintiff will fairly and adequately represent and protect the interests of the Class Members. Plaintiff has retained competent counsel experienced in litigation of class actions, including consumer and data breach class actions, and Plaintiff intends to prosecute this action vigorously. Plaintiff and Class Members have a unified and non-conflicting interest in pursuing the same claims and obtaining the same relief. Therefore, all Class Members will be fairly and adequately represented by Plaintiff and her counsel.

49. *Superiority of Class Action*. A class action is superior to other available methods for the fair and efficient adjudication of the claims alleged in this action. The adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudications of the asserted claims. There will be no difficulty in the management of this action as a class action, and the disposition of the claims of the Class Members in a single action will provide substantial benefits to all parties and to the Court. Damages for any individual Class Member are likely insufficient to justify the cost of individual litigation so that, in the absence of class treatment, Defendants' violations of law inflicting substantial damages in the aggregate would go un-remedied.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

50. Class certification is also appropriate because Defendants have acted or refused to act on grounds generally applicable to the Class Members, such that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

FIRST CAUSE OF ACTION

(Violation of the California Consumer Privacy Act ("CCPA"),

Cal. Civ. Code § 1798.150 *et seq*.)

51. Plaintiff repeats and incorporates by reference each and every allegation contained in paragraphs 1 through 50, inclusive, of this Complaint as if set forth fully herein.

52. Under Cal. Civ. Code § 1798.150(a)(1), "Any consumer whose nonencrypted and nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following:

(A) To recover damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater.

(B) Injunctive or declaratory relief.

(C) Any other relief the court deems proper."

53. Plaintiff and the Class Members provided to Defendants its nonencrypted and nonredacted personal information as defined in § 1798.81.5 in the form of their PII.

54. Plaintiff and the Class Members' PII was subject to an unauthorized access and exfiltration when it was stolen by hackers and posted on the dark web for sale.

55. The unauthorized access, exfiltration, theft, and disclosure of Plaintiff and the Class Members' PII was a result of Walmart's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information. A scan of Walmart's domains using OWASP ZAP resulted in the exposure of six major vulnerabilities, which include:

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

- Private IP addresses being disclosed in the public website code.
- Forty-four instances of password autocomplete enabled.
- The cookie "No HttpOnlyFlag" being set, which means that cookies can be accessed by scripts or malware on the client machine.
- 8,615 instances of XSS protection not enabled.
- 100,061 instances of Cross Domain JavaScript source file inclusion.
- 93,060 instances of a cookie without the secure flag being set.

56. An OWASP Zap scan of http://grocery.walmart.com and the IP address for Walmart photos revealed similar vulnerabilities on those websites.

57. After scanning less than 2% of the Walmart website using the Vega vulnerability scanner, 228 high ranking vulnerabilities materialized. These vulnerabilities include the integer overflow vulnerability, and numbers exposed which appeared to be social security numbers and credit card numbers. Vega also found seven instances where local paths were revealed, which can allow hackers to obtain sensitive information about the server environment.

58. A scan using the Nessus PCI tool scan revealed 20 PCI vulnerabilities, each ranked as high, and identified the following severe issues, each of which would be considered to be an "automatic failure" according to the PCI DSS Approved Scanning Vendors Program Guide (version 3.1):

- Vulnerabilities with a CVSS base score greater than or equal to 4.0;
- Unsupported operating systems;
- Internet reachable database servers;
- Presence of built-in or default accounts;
- Unrestricted DNS Zone transfers;
- Unvalidated parameters leading to SQL injection attacks;
- Cross-Site Scripting (XSS) flaws;
- Directory traversal vulnerabilities;
- HTTP response splitting/header injection;
- Detection of backdoor applications (malware, trojan horses, rootkits, backdoors)

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

- Use of older, insecure SSL/TLS versions
- Use of anonymous key exchange protocols (such as anonymous Diffe-Hellman in SSL/TLS);
- Scan Interference.

59. The Nessus PCI scan also located three problems with Walmart.com's SSL/TLS certificates. SSL/TLS stands for Secure Sockets Layer/Transport Layer Security and is how websites encrypt data transmissions. SSL/TLS utilizes digital certificates to encrypt data. Security flaws in SSL/TLS certificates make all transmissions vulnerable, including transmissions of credit card information and account details.

60. The Nessus PCI scan identified the following problems with Walmart.com's SSL/TLS certificates: SSL certificate cannot be trusted, SSL certificate with wrong hostname, and SSL self-signed certificate. Each of these problems means that data transmissions on the website are vulnerable.

61. The Nessus PCI scan also revealed that Defendant is using an outdated protocol, TLS Version 1.1, which is technology that was replaced 12 years ago and has known weaknesses.

62. Under Walmart's duty to protect the PII, it was required to institute reasonable security measures on its website to deter hacks. These vulnerabilities show that Walmart has breached that duty.

63. Plaintiff has suffered monetary injury in fact as a direct and proximate result of the acts committed by Defendants, as alleged herein, in an amount to be proven at trial, but in excess of the minimum jurisdictional amount of this Court.

SECOND CAUSE OF ACTION

(Negligence)

64. Plaintiff repeats and incorporates by reference each and every allegation contained in paragraphs 1 through 63, inclusive, of this Complaint as if set forth fully herein.

65. Defendants owed Plaintiff and the Class Members, as customers, a duty of care in the handling of PII, which duty included keeping that PII safe and preventing disclosure of that PII to all unauthorized third parties. This duty of care existed independently of Defendants'

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

contractual duty to Plaintiff and the Class Members. Under the CCPA, the Federal Trade Commission ("FTC") Guidelines, and other sources of industry-wide standards, Defendants must incorporate adequate measures to safeguard and protect the PII.

66. As noted, the CCPA creates a duty for all businesses in California to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information.

67. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business.[4] Among other things, the guidelines note businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[5]

68. Additionally, the FTC recommends that companies limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[6]

69. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U.S.C.

[4] Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personalinformation.pdf (last visited Nov. 22, 2019).

[5] *Id.*

[6] Federal Trade Commission, *Start With Security: A Guide for Business* (Jun. 2015) https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

§ 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[7]

70. Additional industry guidelines which provide a standard of care can be found in the National Institute of Standards and Technology's ("NIST's") Framework for Improving Critical Infrastructure Cybersecurity, available at https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf. Among other guideposts, the NIST's framework identifies seven steps for establishing or improving a cybersecurity program (section 3.2). Those steps are:

> *Step 1: Prioritize and Scope*. The organization identifies its business/mission objectives and high-level organizational priorities. With this information, the organization makes strategic decisions regarding cybersecurity implementations and determines the scope of systems and assets that support the selected business line or process. The Framework can be adapted to support the different business lines or processes within an organization, which may have different business needs and associated risk tolerance. Risk tolerances may be reflected in a target Implementation Tier.
>
> *Step 2: Orient*. Once the scope of the cybersecurity program has been determined for the business line or process, the organization identifies related systems and assets, regulatory requirements, and overall risk approach. The organization then consults sources to identify threats and vulnerabilities applicable to those systems and assets.
>
> *Step 3: Create a Current Profile*. The organization develops a Current Profile by indicating which Category and Subcategory outcomes from the Framework Core are currently being achieved. If an outcome is partially achieved, noting this fact will help support subsequent steps by providing baseline information.

///

///

[7] Federal Trade Commission, *Privacy and Security Enforcement: Press Releases* https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-securityenforcement (last visited Nov. 22, 2019).

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

Step 4: Conduct a Risk Assessment. This assessment could be guided by the organization's overall risk management process or previous risk assessment activities. The organization analyzes the operational environment in order to discern the likelihood of a cybersecurity event and the impact that the event could have on the organization. It is important that organizations identify emerging risks and use cyber threat information from internal and external sources to gain a better understanding of the likelihood and impact of cybersecurity events.

Step 5: Create a Target Profile. The organization creates a Target Profile that focuses on the assessment of the Framework Categories and Subcategories describing the organization's desired cybersecurity outcomes. Organizations also may develop their own additional Categories and Subcategories to account for unique organizational risks. The organization may also consider influences and requirements of external stakeholders such as sector entities, customers, and business partners when creating a Target Profile. The Target Profile should appropriately reflect criteria within the target Implementation Tier.

Step 6: Determine, Analyze, and Prioritize Gaps. The organization compares the Current Profile and the Target Profile to determine gaps. Next, it creates a prioritized action plan to address gaps – reflecting mission drivers, costs and benefits, and risks – to achieve the outcomes in the Target Profile. The organization then determines resources, including funding and workforce, necessary to address the gaps. Using Profiles in this manner encourages the organization to make informed decisions about cybersecurity activities, supports risk management, and enables the organization to perform cost-effective, targeted improvements.

Step 7: Implement Action Plan. The organization determines which actions to take to address the gaps, if any, identified in the previous step and then adjusts its current cybersecurity practices in order to achieve the Target Profile. For further guidance, the Framework identifies example Informative References regarding the

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

> Categories and Subcategories, but organizations should determine which standards, guidelines, and practices, including those that are sector specific, work best for their needs.

71. The PCI Data Security Standard ("DSS"), which includes a library of documents available at https://www.pcisecuritystandards.org/document_library?category=educational_resources&document=pci_dss_large_org, is also a source of duties of care applicable to Defendant. The PCI DSS sets forth specific security standards applicable to all businesses which process major credit cards, including Defendant. Included in the documents in the PCI DSS library is a document titled Best Practices for Maintaining PCI DSS Compliance, *available at* https://www.pcisecuritystandards.org/documents/PCI_DSS_V2.0_Best_Practices_for_Maintaining_PCI_DSS_Compliance.pdf?agreement=true&time=1591897283857. The entire document establishes a framework for obtaining and maintaining PCI DSS compliance, thereby establishing duties of care applicable to Defendant.

72. In addition to the PCI DSS library of compliance documents, there is the Requirements and Security Assessment itself, https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf?agreement=true&time=1591898978871, which sets forth specific requirements which a company must meet if it is to process major credit cards, as Defendant does. This document establishes numerous detailed duties which applied to Defendant, including requirement 6.5.7, which concerns cross-site scripting:

> *6.5.7*: Examine software-development policies and procedures and interview responsible personnel to verify that XSS is addressed by coding techniques that include:
>
> • Validating all parameters before inclusion;
>
> • Utilizing context-sensitive escaping.

73. Other statutory duties can be found in California's Customer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification).

///

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

74. In addition to their obligations under federal regulations and industry standards, Defendants owed a duty to Plaintiff and the Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in their possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendants owed a duty to Plaintiff and the Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that their computer systems and networks, and the personnel responsible for them, adequately protected the PII of Plaintiff and the Class Members.

75. Defendants owed a duty to Plaintiff and the Class Members to design, maintain, and test their computer system to ensure that the PII in Defendants' possession was adequately secured and protected.

76. Defendants owed a duty to Plaintiff and the Class Members, to create and implement reasonable data security practices and procedures to protect the PII in their possession, including adequately training their employees and others who accessed PII within their computer systems on how to adequately protect PII.

77. Defendants owed a duty to Plaintiff and the Class Members to implement processes that would detect a breach of their data security systems in a timely manner.

78. Defendants owed a duty to Plaintiff and the Class Members to act upon data security warnings and alerts in a timely fashion.

79. Defendants owed a duty to Plaintiff and the Class Members to disclose if their computer systems and data security practices were inadequate to safeguard individuals' PII from theft because such an inadequacy would be a material fact in the decision to purchase insurance or other health care services from Defendants' or to entrust PII with Defendants.

80. Defendants owed a duty to Plaintiff and the Class Members to disclose in a timely and accurate manner when data breaches occurred.

81. Defendants owed a duty of care to Plaintiff and the Class Members because they were foreseeable and probable victims of any inadequate data security practices. Defendants

///

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

collected PII from Plaintiff and the Class Members directly. Defendants knew that a breach of its data systems would cause Plaintiff and the Class Members to incur damages.

82. Defendants breached their duties of care to safeguard and protect the PII which Plaintiff and the Class Members entrusted to them. Defendants adopted inadequate safeguards to protect the PII, and, as shown, failed to adopt industry-wide standards set forth above in their supposed protection of the PII. Defendants failed to design, maintain, and test their computer system to ensure that the PII was adequately secured and protected, failed to create and implement reasonable data security practices and procedures, failed to implement processes that would detect a breach of their data security systems in a timely manner, failed to disclose the breach in a timely and accurate manner, and otherwise breached each of the above duties of care by implementing lax security procedures which led directly to the breach.

83. Defendants breached the duties set forth in the CCPA, the FTC guidelines, California's Customer Records Act, Cal. Civ. Code §§ 1798.81.5, 1798.82, the NIST's Framework for Improving Critical Infrastructure Cybersecurity, and the PCI DSS. In violation of the CCPA, Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information. In violation of the FTC guidelines, *inter alia*, Defendants did not protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. In violation of the NIST's Framework, Defendant, inter alia, failed to adopt sufficient resources to identity and address security gaps. And, as shown, Defendant violated the PCI-DSS in at least the following ways, in addition to the other violations listed above:

- Vulnerabilities with a CVSS base score greater than or equal to 4.0;
- Unsupported operating systems;
- Internet reachable database servers;
- Presence of built-in or default accounts;
- Unrestricted DNS Zone transfers;

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

- Unvalidated parameters leading to SQL injection attacks;
- Cross-Site Scripting (XSS) flaws;
- Directory traversal vulnerabilities;
- HTTP response splitting/header injection;
- Detection of backdoor applications (malware, trojan horses, rootkits, backdoors);
- Use of older, insecure SSL/TLS versions;
- Use of anonymous key exchange protocols (such as anonymous Diffe-Hellman in SSL/TLS);
- Scan Interference.

84. Finally, in violation of the California Customer Records Act, Defendants failed to employ reasonable security measures, and failed to timely notify Plaintiff and the Class Members of the breach. Indeed, Defendants have, to date, failed to notify its customers of the breach.

85. As a direct and proximate result of Defendants' failure to adequately protect and safeguard the PII, Plaintiff and the Class members suffered damages. Plaintiff and the Class Members were damaged because their PII was accessed by third parties, resulting in increased risk of identity theft and theft of property, and for which Plaintiff and the Class members were forced to adopt costly and time-consuming preventive and remediating efforts. Plaintiff and the Class Members were also damaged in that they paid for goods sold by Defendants in an amount that they would have refused to pay had they known that Defendants would not protect their PII. These damages were magnified by the passage of time because Defendants failed to notify their customers of the data breach.

86. Plaintiff has suffered monetary injury in fact as a direct and proximate result of the acts of negligence committed by Defendants as alleged herein in an amount to be proven at trial but in excess of the minimum jurisdictional amount of this Court.

///

///

///

///

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

THIRD CAUSE OF ACTION

(Violation of the Unfair Competition Law ("UCL"),

Cal. Bus. & Prof. Code § 17200, *et. seq.*)

87. Plaintiff repeats and incorporates by reference each and every allegation contained in paragraphs 1 through 86, inclusive, of this Complaint as if set forth fully herein.

88. By their actions and conduct as alleged herein, Defendants have committed one or more acts of unfair competition within the meaning of the UCL, Cal. Bus. & Prof. Code § 17200, that constitute unfair, unlawful and/or fraudulent business practices as those terms are defined under California law.

89. Defendants' business practices are unfair under the UCL because Defendants have acted in a manner that is immoral, unethical, oppressive, unscrupulous and/or substantially injurious to Plaintiff and the Class Members. The exposure of PII to third parties is substantially injurious because of the significant harm that can result to the customer at the hand of those third parties, and the protective measures that the customer must undertake as a direct result of this exposure. Further, the impact of the practice against Plaintiff and the Class Members far outweighs any possible justification or motive on the part of Defendant. Plaintiff and the Class Members could not reasonably have avoided this injury because they relied upon Defendant's promises to protect and safeguard the PII from disclosure, as all consumers must who participate in today's largely electronic market. Finally, Defendants have committed an unfair act by failing to notify its customers of the breach whatsoever.

90. Defendants' failure to safeguard and protect Plaintiff's and the Class Members' PII is violative of public policy as expressed in the CCPA, the FTC publications, including, Protecting Personal Information: A Guide for Business, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personalinformation.pdf (last visited Nov. 22, 2019), the NIST's Framework for Improving Critical Infrastructure Cybersecurity, and the PCI DSS. These regulations and guidelines set forth a clear public policy that companies such as Walmart take appropriate measures to prevent the exposure of customers' PII to hackers, measures which, as shown *supra*, were not taken by Defendants here.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

91. Defendants' business practices are also unfair because they significantly threaten or harm competition. Participation in today's credit economy is predicated on the security of the PII of the participants in that economy, in the sense that PII is an asset of the individual which, if lost to him or her, jeopardizes his or her very ability to maintain capital. Competitive economic activity cannot exist where PII goes unprotected.

92. Defendants' business practices are unlawful under the UCL because Defendants have violated the CCPA, the FTC Act, and California's Customer Records Act, Cal. Civ. Code §§ 1798.81.5 and 1798.82. In violation of the CCPA, Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information. Defendants' conduct also constituted an unfair or deceptive practice under the FTC Act because it "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." 15 U.S.C. 45(n). Consumers cannot avoid the injury themselves because they are not informed of the severe vulnerabilities presented by the website. There is no benefit to consumers or competition to a vulnerable website, so the injury cannot be outweighed by any such countervailing benefit. In violation of the Customer Records Act, Defendant failed to institute reasonable security measures, and failed to notify Plaintiff and the Class Members of the breach whatsoever.

93. Plaintiff has suffered monetary injury in fact as a direct and proximate result of the acts of unfair competition committed by Defendants, as alleged herein, in an amount to be proven at trial, but in excess of the minimum jurisdictional amount of this Court. Plaintiff suffered a monetary injury when he was forced to purchase credit monitoring services and undertake other efforts to reduce the risk of identity theft from the security breach. These are direct pecuniary losses which are attributable to Defendant's violation of the UCL.

94. Plaintiff also suffered a monetary injury because he did not receive the benefit of his bargain with Defendants, through which he agreed to pay for goods with the understanding that his payment information would be protected by Defendants. Plaintiff would not have paid

///

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

the price he agreed to pay for the goods if he had known that Defendants would not protect his PII.

95. Plaintiff also suffered a monetary injury when he lost the value of his PII, which is a real asset worth real money. Plaintiff's PII, now that it has been exposed to hackers, is no longer worth the price that Plaintiff could have obtained for it on the market.

FOURTH CAUSE OF ACTION

(Breach of Express Contract)

96. Plaintiff repeats and incorporates by reference each and every allegation contained in paragraphs 1 through 95 inclusive, of this Complaint as if set forth fully herein.

97. Defendants entered into an express contract with Plaintiff and the Class Members, pursuant to which they provided Defendants with their PII, and Defendants sold them goods. This contract incorporated Walmart's Privacy Policy, which Walmart posts on its website at https://corporate.walmart.com/privacy-security/walmart-privacy-policy. The privacy policy promises that Walmart will only share the PII with specified persons and entities, none of which are the hackers who obtained the PII in this case.

98. Plaintiffs and the Class Members performed everything that they were required to do under the contract by supplying their PII and paying for the goods in question. All conditions required for Defendant's performance have occurred or were excused.

99. The Privacy Policy states, "We will not share your personal information outside of our corporate family of companies, except in the following circumstances," and proceeds to list eight categories of recipients, none of which were the hackers in this case. (*Id*.)

100. Further, the Privacy Policy promises that Defendants will adopt reasonable security measures to protect the data in its possession, stating:

> How Do We Secure Your Personal Information?
>
> We recognize the importance of maintaining the security of our customers' personal information. ***We use reasonable security measures, including physical, administrative, and technical safeguards to protect your personal information.***
>
> We have a team of associates who are responsible for helping to protect the security of your information. ***Whether you are shopping on our websites, through***

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

> ***our mobile services, or in our stores, we use reasonable security measures, including physical, administrative, and technical safeguards***. These measures may include physical and technical security access controls or other safeguards, information security technologies and policies, procedures to help ensure the appropriate disposal of information, and training programs.

101. Defendants breached these promises. As shown, Defendants allowed hackers to obtain the PII, and did not limit its dissemination to the parties set forth in the Privacy Policy. Defendant also failed to adopt reasonable security measures to protect the data, as illustrated by the innumerable security vulnerabilities its website exhibits.

102. As a result of these breaches, Plaintiff and the Class Members were damaged. Plaintiff and the Class Members' PII is being sold by nefarious individuals on the dark web. As a result, Plaintiff and the Class Members have been forced to incur out of pocket costs for credit monitoring, and to take time and effort to cancel credit cards and freeze accounts. Plaintiff and the Class Members have also lost the benefit of their bargain. Plaintiff and the Class Members agreed to purchase goods and provide their PII to Defendants with the understanding that their PII would be protected. Had Plaintiff and the Class Members known that their PII would not be protected, they would not have agreed to pay the price which they contracted for in exchange for the goods. Plaintiff and the Class Members also face a significant risk that their PII will be stolen, that they will lose money, and that their identities will be stolen as a result of the breach. That risk only increases as time passes and no action is taken. Finally, Plaintiff and the Class Members have lost the value of their PII, which has a real market value.

103. Plaintiff and the Class Members' losses were caused by Defendants' breach. By allowing the hackers to obtain the PII, Defendants caused Plaintiff and the Class Members to incur out-of-pocket expenses, lose the benefit of their bargain, incur the risk of identity and property theft, and lose the value of their PII. By failing to institute reasonable measures to protect the data, each of these categories of damages were also caused, because the hackers breached Defendants' system and Plaintiffs' and the Class Members' computers and accounts due to the vulnerabilities on the website.

///

///

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

104. Plaintiff has suffered monetary injury in fact as a direct and proximate result of the acts committed by Defendants, as alleged herein, in an amount to be proven at trial, but in excess of the minimum jurisdictional amount of this Court.

FIFTH CAUSE OF ACTION

(Breach of Implied Contract)

105. Plaintiff repeats and incorporates by reference each and every allegation contained in paragraphs 1 through 104, inclusive, of this Complaint as if set forth fully herein.

106. Defendants and Plaintiff and the Class Members entered an implied contract governing the use and protection of PII when Plaintiff and the Class Members supplied their PII in order to purchase goods from Defendants. Plaintiffs and the Class Members performed everything that they were required to do under the contract by supplying their PII and paying for the goods in question. All conditions required for Defendants' performance have occurred or were excused.

107. This contract was manifested in the conduct of the parties. By agreeing to take Plaintiff's and the Class Members' PII into its possession, Defendants impliedly agreed to protect that PII from hackers, who were known to attempt to steal PII by hacking entities which possess it, to adopt reasonable measures to protect the PII from hackers, and to timely notify Plaintiff and the Class Members of a data breach should one occur. Defendants knew, or had reason to know, that by taking the PII, they were engaging in conduct that would lead Plaintiff and the Class Members to believe that Defendants would protect that data from exposure to hackers, due to the known risk of hacking, which was understood by both parties to the contract. Other conduct which gives rise to this contractual agreement is Defendants' adoption of passwords through which Plaintiff and the Class Members ostensibly kept their information private, the posting of a Privacy Policy, and tips to protect personal data, on Defendants' website.

108. Defendants breached these promises. As shown, Defendants allowed hackers to obtain the PII. Defendants also failed to adopt reasonable security measures to protect the data, as illustrated by the innumerable security vulnerabilities its website exhibits. Finally, Defendants failed to notify its customers of the data breach whatsoever.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

109. As a result of these breaches, Plaintiff and the Class Members were damaged. Plaintiff and the Class Members' PII is being sold by nefarious individuals on the dark web. As a result, Plaintiff and the Class Members have been forced to incur out of pocket costs for credit monitoring, and to take time and effort to cancel credit cards and freeze accounts. Plaintiff and the Class Members have also lost the benefit of their bargain. Plaintiff and the Class Members agreed to purchase goods and provide their PII to Defendants with the understanding that their PII would be protected. Had Plaintiff and the Class Members known that their PII would not be protected, they would not have agreed to pay the price which they contracted for in exchange for the goods. Plaintiff and the Class Members also face a significant risk that their PII will be stolen, that they will lose money, and that their identities will be stolen as a result of the breach. That risk only increases as time passes and no action is taken. Finally, Plaintiff and the Class Members have lost the value of their PII, which has a real market value.

110. Plaintiff and the Class Members' losses were caused by Defendants' breach. By allowing the hackers to obtain the PII, Defendant caused Plaintiff and the Class Members to incur out-of-pocket expenses, lose the benefit of their bargain, incur the risk of identity and property theft, and lose the value of their PII. By failing to institute reasonable measures to protect the data, each of these categories of damages were also caused, because the hackers breached Defendants' system and Plaintiffs' and the Class Members' computers and accounts due to the vulnerabilities on the website.

111. Plaintiff has suffered monetary injury in fact as a direct and proximate result of the acts committed by Defendants, as alleged herein, in an amount to be proven at trial, but in excess of the minimum jurisdictional amount of this Court.

SIXTH CAUSE OF ACTION

(Breach of the Implied Covenant of Good Faith and Fair Dealing)

112. Plaintiff repeats and incorporates by reference each and every allegation contained in paragraphs 1 through 111, inclusive, of this Complaint as if set forth fully herein.

113. Plaintiff and the Class Members entered contracts with Defendants for the sale of goods, which incorporated the Privacy Policy, and which also included the implied terms that

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

Defendant would not expose the PII to hackers and that Defendants would take reasonable measures to protect the PII.

114. In these contracts, as in every contract, there was an implied covenant of good faith and fair dealing. This implied promise means that each party will not do anything to unfairly interfere with the right of any other party to receive the benefits of the contract. Good faith means honesty of purpose without any intention to mislead or to take unfair advantage of another, that is, being faithful to one's duty or obligation.

115. Plaintiffs and the Class Members performed everything that they were required to do under the contract by supplying their PII and paying for the goods in question. All conditions for Defendants' performance have occurred or were excused.

116. Defendants failed to protect the PII from exposure to hackers, and failed to adopt reasonable measures to protect the PII, operating a website with numerous security flaws as shown above. Defendants also failed to notify Plaintiff and the Class Members of the breach, so that they could make reasonable efforts to protect their identities and property.

117. By doing so, Defendants did not act fairly and in good faith. Good faith and fairness required Defendants to protect the PII from hackers, including by adopting reasonable measures. Consumers must count on companies who collect their PII to protect that PII in order to facilitate commercial transactions, which increasingly occur over the internet.

118. As a result of this conduct, Plaintiff and the Class Members were damaged. Plaintiff and the Class Members' PII is being sold by nefarious individuals on the dark web. As a result, Plaintiff and the Class Members have been forced to incur out of pocket costs for credit monitoring, and to take time and effort to cancel credit cards and freeze accounts. Plaintiff and the Class Members have also lost the benefit of their bargain. Plaintiff and the Class Members agreed to purchase goods and provide their PII to Defendants with the understanding that their PII would be protected. Had Plaintiff and the Class Members known that their PII would not be protected, they would not have agreed to pay the price which they contracted for in exchange for the goods. Plaintiff and the Class Members also face a significant risk that their PII will be stolen, that they will lose money, and that their identities will be stolen as a result of the breach. That

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

risk only increases as time passes and no action is taken. Finally, Plaintiff and the Class Members have lost the value of their PII, which has a real market value.

119. Plaintiff has suffered monetary injury in fact as a direct and proximate result of the acts committed by Defendants, as alleged herein, in an amount to be proven at trial, but in excess of the minimum jurisdictional amount of this Court.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Class, prays for relief as follows:

1. For compensatory damages in an amount according to proof at trial;

2. For affirmative injunctive relief mandating that Defendants implement and maintain reasonable security procedures and practices to protect Plaintiff's and Class Members' PII from unauthorized access, destruction, use, modification, or disclosure, and notify Plaintiff and the Class Members of all data breaches which have occurred;

3. For costs of suit and litigation expenses;

4. For attorneys' fees under the common fund doctrine and all other applicable law; and

5. For such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of himself and all others similarly situated, hereby demands a jury trial for all claims so triable.

Dated: July 10, 2020

Respectfully submitted,

Thiago M. Coelho
Justin F. Marquez
Robert Dart
WILSHIRE LAW FIRM

Attorneys for Plaintiff and the proposed class

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137